EXHIBIT A

KAZEROUNI LAW GROUP, APC
Abbas Kazerounian, Esq. (SBN 249203)
ak@kazlg.com
Mona Amini (SBN 296829)
mona@kazlg.com
245 Fischer Avenue, Unit D1
Costa Mesa, California 92626
Telephone: (800) 400-6808
Facsimile: (800) 520-5523

BLOOD HURST & O'REARDON, LLP
Timothy G. Blood, Esq. (SBN 149343)
tblood@bholaw.com
Jennifer L. MacPherson, Esq. (SBN 202021)
jmacpherson@bholaw.com
501 West Broadway, Suite 1490
San Diego, CA 92101
Telephone: (619) 338-1100
Facsimile: (619) 338-1101

Attorneys for Plaintiff
Leslie May and the putative class

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF CONTRA COSTA – COMPLEX CIVIL

LESLIE MAY, individually, and on behalf of all others similarly situated,

Plaintiff,

vs.

ARTHUR J. GALLAGHER & CO.; and DOES 1-50, inclusive,

Defendant(s).

Case No.: C21-01705

CLASS ACTION COMPLAINT FOR VIOLATIONS OF:

1. CALIFORNIA CONSUMER PRIVACY ACT OF 2018, CAL. CIV. CODE §§ 1798.100, *et seq.*;
2. CALIFORNIA UNFAIR COMPETITION LAW, CAL. BUS. & PROF. CODE §§ 17200, *et. seq.*; and
3. BREACH OF CONTRACT

JURY TRIAL DEMANDED

//

//

//

Plaintiff LESLIE MAY ("Plaintiff"), individually and on behalf of the general public and all others similarly situated (the "Class members"), by and through her attorneys, upon personal knowledge as to facts pertaining to herself and on information and belief as to all other matters, brings this class action against Defendant ARTHUR J. GALLAGHER & CO. ("Gallagher" or "Defendant") and DOES 1-50, inclusive, and alleges as follows:

NATURE OF THE CASE

1. This is a data breach class action arising out of Defendant's failure to implement and maintain reasonable security practices to protect consumers' sensitive personal information. Defendant is a global leader in insurance, risk management and consulting services that has an international group of partners in more than 150 countries that provide cost-effective, client-centric, and expertise-driven risk management solutions.[1] For their business purposes, Defendant obtains, stores, and transmits personally identifiable information ("PII") from customers, including but not limited to their customers' Social Security number or tax identification number, driver's license, passport or other government identification number, date of birth, username and password, employee identification number, financial account or credit card information, electronic signature, medical treatment, claim, diagnosis, medication or other medical information, health insurance information, medical record or account number, and biometric information.

2. On September 26, 2020, Defendant became of aware of a ransomware event which impacted its internal systems. Defendant launched an investigation with the assistance of third-party cybersecurity and forensic specialists who determined that an unknown unauthorized party accessed or acquired data contained within certain segments of Defendant's network over a three-month period between June 3, 2020 and September 26, 2020.

3. On May 24, 2021, Defendant's investigation confirmed that that one or more of the following types of information associated with certain individuals were present on impacted systems and subject to access or acquisition by the unknown actor: Social Security number or tax identification number, driver's license, passport or other government identification number, date of

[1] https://www.ajg.com

birth, username and password, employee identification number, financial account or credit card information, electronic signature, medical treatment, claim, diagnosis, medication or other medical information, health insurance information, medical record or account number, and biometric information (the "Data Breach"). Although the exact number of affected customers is presently unknown, based upon information and belief at least 226,920 customers have been affected by the Data Breach nationwide. The Data Breach occurred between June 3, 2020 and September 26, 2020. However, Defendant only provided notice to Plaintiff and their other customers of the Data Breach on or around July 21, 2021.

1. Although Defendant knew about the Data Breach in September 2020, it waited until nearly a year later until July 21, 2021, to send certain customers letters regarding the Data Breach. Defendant's notice to customers was misleading and inadequate as the notice did not explain the ten-month delay between discovering the breach and notifying affected customers.

2. The Data Breach occurred as a result of Defendant's inadequate cybersecurity, which caused Plaintiff's and Class members' PII to be accessed, exfiltrated, and disclosed to unauthorized persons. This action seeks to remedy these failings. Plaintiff brings this action on behalf of herself and all affected California residents.

3. As set forth in the Prayer for Relief, among other things, Plaintiff seeks, for herself and the Class members damages, including public injunctive relief, and actual damages.

VENUE AND JURISDICTION

4. This Court has jurisdiction over this action pursuant to Cal. Code Civ. Proc. § 410.10 and Cal. Bus. & Prof. Code §§ 17203-17204, 17604. This action is brought as a class action on behalf of Plaintiff and the Class members pursuant to Cal. Code Civ. Proc. § 382.

5. This Court has personal jurisdiction over Defendant because Defendant regularly conducts business in the State of California.

6. Venue is proper in this Court pursuant to Cal. Code Civ. Proc. § 395 and § 395.5 because Defendant regularly conducts business in the State of California, Plaintiff resides in this county, and the unlawful acts or omissions giving rise to this action also occurred or arose in this county.

PARTIES

7. At all relevant times, Plaintiff resided in the State of California.

8. At all relevant times, Defendant conducted business in the State of California.

9. Plaintiff provided her PII to Defendant as part of Defendant's insurance and claims services, including Plaintiff's Social Security number or tax identification number, driver's license, passport or other government identification number, date of birth, username and password, employee identification number, financial account or credit card information, electronic signature, medical treatment, claim, diagnosis, medication or other medical information, health insurance information, medical record or account number, and biometric information. In July 2021, Plaintiff learned that her PII, including her name, Social Security Number, and confidential medical information, including medical diagnosis, medical treatment information, and medical claim information, was accessed, viewed, and/or acquired by unauthorized individuals through the Data Breach.

10. Defendant sent Plaintiff a letter dated July 21, 2021 with the subject "Notice of Data Breach." The letter notified Plaintiff and other similarly situated persons that as a result of a ransomware event impacting is internal systems, an unknown unauthorized party accessed or acquired data contained within certain segments of Defendant's network over a three-month period between June 3, 2020 and September 26, 2020. No details were provided regarding who stole the information in the Data Breach or why there was a delay in the investigation and the notification to affected customers.

11. As a result of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information it collected, maintained, and stored on its servers, network, and/or email system, Plaintiff's PII was accessed, viewed, exfiltrated, stolen and/or otherwise disclosed to unauthorized persons in the Data Breach.

12. Defendant is a corporation formed under the laws of the State of Illinois and headquartered in Rolling Meadows, Illinois. Defendant is a global leader in insurance, risk management and consulting services that has an international group of partners in more than 150

countries that provide cost-effective, client-centric, and expertise-driven risk management solutions.[2]

13. Plaintiff is unaware of the true names and capacities of the Defendant sued herein as DOES 1 through 50, inclusive, and therefore sues this Defendant by such fictitious names pursuant to Cal. Civ. Proc. Code § 474. Plaintiff is informed and believes, and based thereon, alleges that Defendant designated herein is legally responsible in some manner for the unlawful acts and occurrences complained of herein, whether such acts were committed intentionally, negligently, recklessly, or otherwise, and Defendant thereby proximately caused the injuries and damages to Plaintiff and the Class members as herein alleged. Plaintiff will seek leave of Court to amend this complaint to reflect the true names and capacities of Defendant when they have been ascertained and become known.

14. The agents, servants and/or employees of Defendant and each of them acting on behalf of Defendant acted within the course and scope of his, her or its authority as the agent, servant and/or employee of Defendant, and personally participated in the conduct alleged herein on behalf of Defendant with respect to the conduct alleged herein. Consequently, the acts of each Defendant are legally attributable to the other Defendants and all Defendants are jointly and severally liable to Plaintiffs and other similarly situated individuals, for the loss sustained as a proximate result of the conduct of the Defendants' agents, servants and/or employees.

FACTUAL ALLEGATIONS

PII Is a Valuable Property Right that Must Be Protected

15. The California Constitution guarantees every Californian a right to privacy. And PII is a recognized valuable property right.[3] California has repeatedly recognized this property right, most recently with the passage of the California Consumer Privacy Act of 2018.

---

[2] https://www.ajg.com

[3] *See* John T. Soma, et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *2 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

16. In a Federal Trade Commission ("FTC") roundtable presentation, former Commissioner, Pamela Jones Harbour, underscored the property value attributed to PII by observing:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.[4]

17. The value of PII as a commodity is measurable. "PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets."[5] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market" for several years.

18. Companies recognize PII as an extremely valuable commodity akin to a form of personal property. For example, Symantec Corporation's Norton brand has created a software application that values a person's identity on the black market.[6]

19. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals openly post credit card numbers, Social Security numbers, PII and other sensitive information directly on various illicit Internet websites making the information publicly available for other criminals to take and use. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims. In one study, researchers found hundreds of websites displaying stolen PII and other sensitive information. Strikingly, none of these websites were blocked by Google's safeguard filtering mechanism – the "Safe Browsing list."

20. Recognizing the high value that consumers place on their PII, some companies now offer consumers an opportunity to sell this information to advertisers and other third parties. The idea is to give consumers more power and control over the type of information they share – and

---

[4] FTC, *Statement of FTC Commissioner Pamela Jones Harbour* (Remarks Before FTC Exploring Privacy Roundtable) (Dec. 7, 2009), https://www.ftc.gov/public-statements/2009/12/remarks-ftc-exploring-privacy-roundtable.

[5] *See* Soma, *Corporate Privacy Trend, supra*.

[6] Risk Assessment Tool, Norton 2010, www.everyclickmatters.com/victim/assessment-tool.html.

who ultimately receives that information. By making the transaction transparent, consumers will make a profit from the surrender of their PII.[7] This business has created a new market for the sale and purchase of this valuable data.[8]

21. Consumers place a high value not only on their PII, but also on the privacy of that data. Researchers shed light on how much consumers value their data privacy – and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[9]

22. One study on website privacy determined that U.S. consumers valued the restriction of improper access to their PII between $11.33 and $16.58 per website.[10]

23. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

Theft of PII Has Grave and Lasting Consequences for Victims

24. A data breach is an incident in which sensitive, protected, or confidential data has potentially been viewed, stolen, or used by an individual unauthorized to do so. As more consumers rely on the internet and apps on their phone and other devices to conduct every-day transactions, data breaches are becoming increasingly more harmful.

25. Theft or breach of PII is serious. The California Attorney General recognizes that "[f]oundational" to every Californian's constitutional right to privacy is "information security: if

---

[7] Steve Lohr, *You Want My Personal Data? Reward Me for It*, N.Y. Times (July 16, 2010) *available at* https://www.nytimes.com/2010/07/18/business/ 18unboxed.html.

[8] *See* Julia Angwin and Emil Steel, *Web's Hot New Commodity: Privacy*, Wall Street Journal (Feb. 28, 2011) *available at* https://www.wsj.com/articles/SB10001424052748703529004576160764037920274.

[9] Janice Y. Tsai, et al., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study Information Systems Research* 22(2) 254, 254 (June 2011), *available at* https://www.jstor.org/stable/23015560?seq=1# page_scan_tab_contents.

[10] II–Horn, Hann, et al., *The Value of Online Information Privacy: An Empirical Investigation* (Mar. 2003) at table 3, *available at* https://ideas.repec.org/p/wpa/wuwpio/0304001.html (emphasis added).

companies collect consumers' personal data, they have a duty to secure it. An organization cannot protect people's privacy without being able to secure their data from unauthorized access."[11]

26. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use PII to take over existing financial accounts, open new financial accounts, receive government benefits and incur charges and credit in a person's name.[12] As the GAO Report states, this type of identity theft is so harmful because it may take time for the victim to become aware of the theft and can adversely impact the victim's credit rating.

27. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records … [and their] good name." According to the FTC, identity theft victims must spend countless hours and large amounts of money repairing the impact to their good name and credit record.[13]

28. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[14] According to Experian, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[15]

---

[11] California Data Breach Report, Kamala D. Harris, Attorney General, California Department of Justice, February 2016.

[12] *See* GAO, GAO Report 9 (2007) *available at* http:///www.gao.gov/new.items/d07737.pdf.

[13] *See* FTC Identity Theft Website: https://www.consumer.ftc.gov/features/feature-0014-identity-theft.

[14] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

[15] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself?*, EXPERIAN (Sept. 7, 2017), *available at*

29. According to the IBM and Ponemon Institute's 2019 "Cost of a Data Breach" report, the average cost of a data breach per consumer was $150 per record.[16] Other estimates have placed the costs even higher. The 2013 Norton Report estimated that the average cost per victim of identity theft – a common result of data breaches – was $298 dollars.[17] And in 2019, Javelin Strategy & Research compiled consumer complaints from the FTC and indicated that the median out-of-pocket cost to consumers for identity theft was $375.[18]

30. A person whose PII has been compromised may not see any signs of identity theft for years. According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

31. For example, in 2012, hackers gained access to LinkedIn's users' passwords. However, it was not until May 2016, four years after the breach, that hackers released the stolen email and password combinations.[19]

32. It is within this context that Plaintiff and hundreds of thousands of Defendant's customers face imminent risk of identity theft and must now live with the knowledge that their PII is forever in cyberspace and was taken, accessed, and/or viewed by unauthorized persons willing and able to use the information for any number of improper purposes and scams, including making the information available for sale on the dark web or the black market.

---

https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[16] Brook, *What's the Cost of a Data Breach in 2019*, *supra*.

[17] Norton By Symantec, 2013 Norton Report 8 (2013), *available at* https://yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton_raportti.pdf.

[18] Facts + Statistics: *Identity Theft and Cybercrime*, Insurance Information Institute, *available at* https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (citing the Javelin report).

[19] *See* Cory Scott, *Protecting Our Members*, LINKEDIN (May 18, 2016), *available at* https://blog.linkedin.com/2016/05/18/protecting-our-members.

Defendant's Businesses

33. Defendant is a global leader in insurance, risk management and consulting services that has an international group of partners in more than 150 countries that provide cost-effective, client-centric, and expertise-driven risk management solutions.

34. Defendant describes itself as being in the business of assisting individuals and companies with insurance related solutions through insurance placement, risk management, and consulting services. In its role as an insurance broker or agent, Defendant claims to act as a service provider on behalf of its clients and insurance carriers.

35. When Plaintiff and similarly situated customers apply for financing with or through Defendant, they are required to provide Defendant with certain personal information. This personal information includes the customer's name, social security number, date of birth, driver's license and/or other government issued ID containing a photograph, telephone number, healthcare account number, personal bank account information, and health insurance information.

Defendant's Collection of Customers' PII

36. Defendant acknowledges that it obtains, stores and transmits a substantial amount of personal, financial, and medical information from its customers. The type of information is detailed in Defendant's Privacy Policy (last updated December 2019),[20] which states that Defendant collects the following categories of personal information from customers, among others:

- personal details (e.g., name, date of birth);
- contact details (e.g., phone number, email address, postal address or mobile number);
- government issued identification details (e.g., social security and national issuance numbers, passport details)
- health and medical details (e.g., health certificates);
- policy details (e.g., policy numbers and types);
- bank details (e.g., payment details, account numbers and sort codes);
- driving license details;
- online log-in information (e.g., username, password, security question answers);
- information relating to any claims;
- other information from applications or questionnaires;
- information collected automatically (e.g., click stream data, personal information and other data collected using cookies and other device identifying technologies)

[20] *See* Defendant's Privacy Policy, available at https://www.ajg.com/us/privacy-policy

37. Defendant collects personal information from customers directly as well as through third parties such as insurers, consumer reporting agencies, Defendant's affiliated companies, or other third parties in the course of conducting Defendant's business.

38. For California customers, Defendant's Privacy Policy identifies the rights of California residents regarding their personal information pursuant to the California Consumer Privacy Act ("CCPA"). These rights include requesting disclosure of the information collected, the purpose for collecting the information, and any third parties with whom the information is sold or disclosed. Additionally, the rights under the CCPA identified by Defendant's Privacy Policy include requesting deletion of the personal information, opting out of have personal information sold to third parties, and receiving information that identifies any third party that has received personal information.

Defendant's Promises to Safeguard Customer PII

39. Defendant claims it implements "technical, organizational, administrative and physical measures to help ensure a level of security appropriate to the risk to the personal information we collect, use, disclose and process. These measures are aimed at ensuring the on-going integrity and confidentiality of personal information. We evaluate these measures on a regular basis to help ensure the security of the processing. Please be aware that, despite our ongoing efforts, no security measures are perfect or impenetrable."

40. Defendant also promises that it "restrict[s] access to your personal information to those who require access to such information for legitimate, relevant business purposes."

41. Defendant's Terms of Use Agreement expressly references Defendant's Privacy Policy and states the terms and conditions of the Privacy Policy are incorporated into Defendant's Terms of Use.

The Data Breach

42. On July 21, 2021, Defendant sent Plaintiff and other similarly situated customers a letter with the subject line, "Notice of Data Breach" The letter stated that "On September 26, 2020, Gallagher detected a ransomware event impacting our internal systems" and went on to state that "certain information relating to [Plaintiff] was accessed or acquired during this event."

43. Further the letter states that "[o]n May 24, 2021, Gallagher's investigation confirmed that the impacted data included information relating to certain individuals" and it worked through June 23, 2021 to confirm the accuracy of the information for impacted individuals to provide notice to impacted parties such as Plaintiff who received Gallagher's Notice of Data Breach letter.

44. According to Defendant, the information accessed, viewed, and/or acquired by unauthorized individuals through the Data Breach specifically included Plaintiff's PII, including her name, Social Security Number, and confidential medical information, including medical diagnosis, medical treatment information, and medical claim information.

45. Defendant claimed to have immediately launched an investigation with the assistance of third-party cybersecurity and forensic specialists after it detected the ransomware event impacting its internal systems on September 26, 2020. Defendant provided little explanation as to why it took until May 24, 2021 for Defendant's investigation to confirm the data and individuals impacted by the Data Breach.

46. Defendant offered customers access, at no cost, to twenty-four month Kroll identity theft and credit monitoring services.

47. Additionally, Defendant offered a limited number of steps on how to protect against identity theft and fraud. These steps included reviewing account statements and credit reports.

48. For California residents, the letter does not identify the rights of consumers under CCPA and instead says to "[v]isit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft."

Defendant's Notice of Data Breach

49. On July 21, 2021, Defendant sent Plaintiff and other similarly situated customers affected by the Data Breach the "Notice of Data Breach" letter.

50. On June 30, 2021, Defendant reported the Data Breach to the California Attorney General.

51. Pursuant to California Civ. Code § 1798.82(a)(1), data breach notification letters must be sent to residents of California "whose unencrypted personal information was, or is

reasonably believed to have been, acquired by an unauthorized person" due to a "breach of the security of the system[.]"

52. Defendant's sample data breach notification letter was filed with the California Attorney General in accordance with California Civ. Code § 1798.82(f).

53. Plaintiff's and Class members' PII is "personal information" as defined by California Civ. Code § 1798.82(h).

54. California Civ. Code § 1798.82(g) defines "breach of the security of the system" as the "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business."

55. The Data Breach was a "breach of the security of the system" as defined by California Civ. Code § 1798.82(g).

56. Thus, Defendant filed and disseminated its breach notification because Plaintiff's and Class members' unencrypted personal information was accessed and acquired by an unauthorized person or persons as a result of the Data Breach.

57. Defendant's Notice of the Data Breach letter sent to Plaintiff and other putative class members is inadequate and fails to provide sufficient detail. Defendant states only that "[o]n September 26, 2020, Gallagher detected a ransomware event impacting our internal systems" and went on to state that Gallagher's "investigation determined that an unknown party accessed or acquired data contained within certain segments of [Gallagher's] network between June 3, 2020 and September 26, 2020." However, Gallagher's letter failed to give any further detail about the unauthorized access and acquisition of Plaintiff and other similarly situated persons' personal information, including PII and confidential medical information.

58. Defendant's vague description of the Data Breach leaves Plaintiff and Class members at continuing risk. By failing to adequately inform Plaintiff and Class members of all the details surrounding the breach Plaintiff and Class members are unable to adequately protect themselves against identity theft and other damages.

59. Further, Defendant offers Plaintiff and Class members little to assist them with any fall-out from the Data Breach or to advise them of the extent of the potential threat they face as a

result of their sensitive PII being in the hands of criminals. Defendant's offer of a two year subscription to Kroll's credit identity and credit monitoring services is insufficient where Plaintiff and Class members are now at increased risk of identity theft for years to come and the indefinite future as a result of the Data Breach.

60. Defendant also fails to explain why it took over ten months from learning of the ransomware incident in September 2020 to notify Plaintiff and Class members about the Data Breach on or about July 21, 2021. This delayed Plaintiff's and Class members' ability to be fully informed and take necessary precautions to protect themselves from identity theft and other fraud.

Defendant Knew or Should Have Known PII Are High Risk Targets

61. Defendant knew or should have known that PII like the information obtained, maintained and stored on Defendant's servers and network is a high risk target for identity thieves.

62. The Identity Theft Resource Center reported that the business sector had the largest number of breaches in 2018. According to the ITRC this sector suffered 571 data breaches exposing at least 415,233,143 million records in 2018.[21] Further, the ITRC identified "hacking" as the most common form of data breach in 2018, accounting for 39% of data breaches.

63. Prior to the Data Breach, there were many reports of high-profile data breaches that should have put a company like Defendant on high alert and forced it to closely examine their own security procedures, as well as those of third parties with which it did business and gave access to their subscriber PII.

64. In addition, amid the ongoing COVID-19 pandemic, identity theft has soared. Complaints to the Federal Trade Commission more than doubled to 1.38 million from 2019 to 2020, a tally that includes unemployment-benefits fraud.[22] Last year, The Federal Trade Commission (FTC) received more than 394,000 complaints from consumers who said their identities had been

---

[21] Identity Theft Resource Center, *2018 End-of-Year Data Breach Report*, *available at* https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.

[22] https://www.wsj.com/articles/unemployment-benefits-fraud-has-soared-in-the-pandemic-heres-what-to-do-11619688601

"misused" to apply for government benefits, a jump of nearly 3,000% since last year. [23] In addition, there has been a growing wave of arrests and prosecutions involving pandemic relief fraudsters reported by the Department of Justice (DOJ),[24] including using false information on loan applications obtained through identity theft to apply for fraudulent Economic Injury Disaster Loans (EIDL) and Paycheck Protection Program (PPP) loans.

65. As such, Defendant was aware that PII is at high risk of theft, and consequently should have but did not take appropriate and standard measures to protect Plaintiff's and Class members' PII against cyber-security attacks that Defendant should have anticipated and guarded against.

CLASS DEFINITION AND ALLEGATIONS

66. Pursuant to Cal. Code Civ. Proc. § 382 and Cal. Civ. Code § 1781, Plaintiff seeks to represent and intends to certify a class defined as (the "Class"):

> ***All California residents who Defendant and/or its agents sent a "Notice of Data Breach" letter to informing them their personally identifiable information (PII) was subjected to the Data Breach.***

67. Excluded from the Class are: (1) Defendant and its officers, directors, employees, principals, affiliated entities, controlling entities, agents, and other affiliates; (2) the agents, affiliates, legal representatives, heirs, attorneys at law, attorneys in fact, or assignees of such persons or entities described herein; and (3) the Judge(s) assigned to this case and any members of their immediate families.

68. Certification of Plaintiff's claims for classwide treatment is appropriate because Plaintiff can prove the elements of her claims on a classwide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

---

[23] https://www.forbes.com/advisor/personal-finance/identity-theft-unemployment-benefits-fraud/

[24] https://www.jdsupra.com/legalnews/update-the-growing-wave-of-ppp-loan-4854683/

69. The Class members are so numerous and geographically dispersed throughout California that joinder of all Class members would be impracticable. While the exact number of Class members is unknown, Defendant acknowledges the Data Breach, and reports estimate the breach to hundreds of thousands of customers, including Plaintiff and Class members. Plaintiff therefore believes that the Class is so numerous that joinder of all members is impractical.

70. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had her PII compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions committed by Defendant, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

71. There is a well-defined community of interest in the common questions of law and fact affecting Class members. The questions of law and fact common to Class members predominate over questions affecting only individual Class members, and include without limitation:

(a) Whether Defendant had a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the PII it collected from Plaintiff and Class members;

(b) Whether Defendant breached their duty to protect the PII of Plaintiff and each Class member; and

(c) Whether Plaintiff and each Class member are entitled to damages and other equitable relief.

72. Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff is an adequate representative of the Class in that Plaintiff has no interests adverse to or that conflict with the Class she seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

73. A class action is superior to any other available method for the fair and efficient adjudication of this controversy since individual joinder of all Class members is impractical.

Furthermore, the expenses and burden of individual litigation would make it difficult or impossible for the individual members of the Class to redress the wrongs done to them, especially given that the damages or injuries suffered by each individual member of the Class are outweighed by the costs of suit. Even if the Class members could afford individualized litigation, the cost to the court system would be substantial and individual actions would also present the potential for inconsistent or contradictory judgments. By contrast, a class action presents fewer management difficulties and provides the benefits of single adjudication and comprehensive supervision by a single court.

74. Defendant has acted or refused to act on grounds generally applicable to the entire Class, thereby making it appropriate for this Court to grant final injunctive, including public injunctive relief, and declaratory relief with respect to the Class as a whole.

CAUSES OF ACTION

FIRST CAUSE OF ACTION

Violation of the California Consumer Privacy Act of 2018 ("CCPA")
Cal. Civ. Code §§ 1798.100, *et seq.*

75. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

76. As more personal information about consumers is collected by businesses, consumers' ability to properly protect and safeguard their privacy has decreased. Consumers entrust businesses with their personal information on the understanding that businesses will adequately protect it from unauthorized access and disclosure. The California Legislature explained: "The unauthorized disclosure of personal information and the loss of privacy can have devasting effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm."[25]

77. As a result, in 2018, the California Legislature passed the CCPA, giving consumers broad protections and rights intended to safeguard their personal information. Among other things,

---

[25] California Consumer Privacy Act (CCPA) Compliance, https://buyergenomics.com/ccpa-complience/.

the CCPA imposes an affirmative duty on businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected. Defendant failed to implement such procedures which resulted in the Data Breach.

78. It also requires "[a] business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party . . . [to] require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." Cal. Civ. Code § 1798.81.5(c).

79. Section 1798.150(a)(1) of the CCPA provides: "Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

80. Plaintiff and Class members' are "consumer[s]" as defined by Civ. Code § 1798.140(g) because they are "natural person[s] who [are] California resident[s], as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017."

81. Defendant is a "business" as defined by Civ. Code § 1798.140(c) because Defendant:

a. is a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners";

b. "collects consumers' personal information, or on the behalf of which is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information";

c. does business in California; and

d. has annual gross revenues in excess of $25 million; annually buys, receives for the business' commercial purposes, sells or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; or derives 50 percent or more of its annual revenues from selling consumers' personal information.

82. The PII taken in the Data Breach is personal information as defined by Civil Code § 1798.81.5(d)(1)(A) because it contains Plaintiff's and Class members' unencrypted first and last names, Social Security numbers and driver's license numbers, medical information, among other information.

83. Plaintiff's and the putative Class' PII was subject to unauthorized access and exfiltration, theft, or disclosure because their PII, including name and contact information was wrongfully taken, accessed, and viewed by unauthorized third parties.

84. The Data Breach occurred as a result of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect Plaintiff's and Class members' PII. Defendant failed to implement reasonable security procedures to prevent an attack on their server or network, by hackers and to prevent unauthorized access of Plaintiff's and Class members' PII as a result of this attack.

85. Concurrent with the filing of this Complaint, Plaintiff provided Defendant with written notice of its violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1). *See* Ex. A. If Defendant does not cure the violation within 30 days, Plaintiff will amend the complaint to pursue statutory damages as permitted by Civil Code § 1798.150(a)(1)(A).

86. As a result of Defendant's failure to implement and maintain reasonable security procedures and practices that resulted in the Data Breach, Plaintiff seeks actual damages, injunctive relief, including public injunctive relief, and declaratory relief, and any other relief as deemed appropriate by the Court.

SECOND CAUSE OF ACTION

Violation of the California Unfair Competition Law ("UCL")

(Cal. Bus. & Prof. Code §§ 17200, *et seq.*)

87. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

88. The UCL prohibits any "unlawful," "fraudulent" or "unfair" business act or practice and any false or misleading advertising, as those terms are defined by the UCL and relevant case law. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendant engaged in unlawful, unfair and fraudulent practices within the meaning, and in violation of, the UCL.

89. In the course of conducting their business, Defendant committed "unlawful" business practices by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class members' PII, and by violating the statutory and common law alleged herein, including, *inter alia*, California Consumer Privacy Act of 2018 (Cal. Civ. Code §§ 1798.100, *et seq.*) and Article I, Section 1 of the California Constitution (California's constitutional right to privacy) and Civil Code § 1798.81.5. Plaintiff and Class members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

90. Defendant also violated the UCL's unlawful prong by breaching contractual obligations created by their Privacy Policies and by knowingly and willfully or, in the alternative, negligently and materially violating Cal. Bus. & Prof. Code § 22576, which prohibits a commercial website operator from "knowingly and willfully" or "negligently and materially" failing to comply with the provisions of their posted privacy policy. Plaintiff and Class members suffered injury in fact and lost money or property as a result of Defendant's violations of their Privacy Policies.

91. Defendant also violated the UCL by failing to timely notify Plaintiff and Class members pursuant to Civil Code § 1798.82(a) regarding the unauthorized access and disclosure of their PII. If Plaintiff and Class members had been notified in an appropriate fashion, they could have taken precautions to safeguard and protect their PII and identities.

92. Defendant's above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair" business acts and practices in violation of the UCL in that Defendant's wrongful conduct is substantially injurious to consumers, offends legislatively-declared public policy, and is immoral, unethical, oppressive, and unscrupulous. Defendant's practices are also contrary to legislatively declared and public policies that seek to protect PII and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws such as the CCPA, Article I, Section 1 of the California Constitution, and the FTC Act (15 U.S.C. § 45). The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

93. Plaintiff and Class members suffered injury in fact and lost money or property as a result of Defendant's violations of their Privacy Policies and statutory and common law in that a portion of the money Plaintiff and Class members paid for Defendant's products and services went to fulfill the contractual obligations set forth in their Privacy Policy, including maintaining the security of their PII, and Defendant's legal obligations and Defendant failed to fulfill those obligations.

94. The UCL also prohibits any "fraudulent business act or practice." Defendant's above-described claims, nondisclosures and misleading statements were false, misleading and likely to deceive the consuming public in violation of the UCL.

95. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and their violations of the UCL, Plaintiff and Class members have suffered injury in fact and lost money or property as a result of Defendant's unfair and deceptive conduct. Such injury includes

paying for a certain level of security for their PII but receiving a lower level, paying more for Defendant's products and services than they otherwise would have had they known Defendant was not providing the reasonable security represented in their Privacy Policy and as in conformance with their legal obligations. Defendant's security practices have economic value in that reasonable security practices reduce the risk of theft of customer's PII.

96. Plaintiff and Class members have also suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate and the continuing increased risk of identity theft and identity fraud – risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII, (iv) statutory damages under the CCPA, (v) deprivation of the value of their PII for which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring financial accounts, and mitigating damages.

97. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiff, therefore, on behalf of herself, Class members, and the general public, also seeks restitution and an injunction, including public injunctive relief prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant to modify their corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the PII entrusted to it, as well as all other relief the Court deems appropriate, consistent with Bus. & Prof. Code § 17203.

THIRD CAUSE OF ACTION

Breach of Contract

98. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

99. Plaintiff and Class members entered into express contracts with Defendant as set forth in their Terms of Use and Privacy Policy that included Defendant's promise to protect

nonpublic personal information given to Defendant or that Defendant gathered on their own, from disclosure, as set forth in Defendant's Privacy Policy, which was posted on its website.

100. Plaintiff and Class members performed their obligations under the contracts when they provided their PII to Defendant in relation to their purchase of insurance products or services from Defendant.

101. By allowing unauthorized users to gain access to Plaintiff's and Class members' PII through the Data Breach, Defendant breached these contractual obligations. As a result, Defendant failed to comply with their own policies, including their Privacy Policy, and applicable laws, regulations and industry standards for data security and protecting the confidentiality of PII. Defendant's breach of contract also violated California Business and Professions Code § 22576, which prohibits a commercial website operator from "knowingly and willfully" or "negligently and materially" failing to comply with the provisions of their posted privacy policy.

102. By failing to fulfill their contractual obligations under their Terms of Use and Privacy Policy, Defendant failed to confer on Plaintiff and Class members the benefit of the bargain, causing them economic injury.

103. As a direct and proximate result of the Data Breach, Plaintiff and Class members have been harmed and have suffered, and will continue to suffer, damages and injuries.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all members of the Class respectfully requests that (i) this action be certified as a class action, (ii) Plaintiff be designated representative of the Class, and (iii) Plaintiff's undersigned counsel be appointed as Class Counsel. Plaintiff, on behalf of herself and members of the Class further requests that upon final trial or hearing, judgment be awarded against Defendant for:

(i) actual and punitive damages to be determined by the trier of fact;

(ii) statutory damages;

(iii) equitable relief, including restitution;

(iv) appropriate injunctive relief;

(v) attorneys' fees and litigation expenses under Code of Civil Procedure § 1021.5 and other applicable law;

(vi) costs of suit;

(vii) pre- and post-judgment interest at the highest legal rates applicable; and

(viii) any such other and further relief the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of herself individually and the putative class, hereby demands a jury trial on all issues so triable.

Dated: August 13, 2021

Respectfully submitted,

KAZEROUNI LAW GROUP, APC

By: _____

Abbas Kazerounian, Esq.
Mona Amini, Esq.
245 Fischer Avenue, Unit D1
Costa Mesa, California 92626
Telephone: (800) 400-6808
Facsimile: (800) 520-5523
ak@kazlg.com
mona@kazlg.com

BLOOD HURST & O'REARDON, LLP
Timothy G. Blood, Esq. (SBN 149343)
Jennifer L. MacPherson, Esq. (SBN 202021)
501 West Broadway, Suite 1490
San Diego, CA 92101
Telephone: (619) 338-1100
Facsimile: (619) 338-1101
tblood@bholaw.com
jmacpherson@bholaw.com

Attorneys for Plaintiff Leslie May and the putative class

EXHIBIT A

KAZEROUNI LAW GROUP, APC

245 Fischer Avenue, Unit D1
Costa Mesa, California 92626
Telephone: (800) 400-6808
Facsimile: (800) 520-5523
www.kazlg.com

August 16, 2021

VIA CERTIFIED MAIL
Arthur J. Gallagher & Co.
2850 Golf Road
Rolling Meadows, IL 60008

Re: Leslie May v. Arthur J. Gallagher & Co.

To Whom It May Concern:

We represent Plaintiff Leslie May ("Plaintiff") and all other similarly situated consumers in a putative class action against Arthur J. Gallager & Co. ("Defendant" or "Gallagher") related to *inter alia*, Defendant's failure to provide adequate security for Plaintiff's and the proposed class members' personal information, which resulted in the unauthorized access, acquisition, and disclosure of this information (the "Data Breach"). Based upon information and belief the Data Breach occurred between June 3, 2020 and September 26, 2020, as stated in Defendant's "Notice of Data Breach" letter dated July 21, 2021.

The full claims, including the facts and circumstances surrounding these claims are detailed in Plaintiff's Class Action Complaint, a copy of which is attached and incorporated by reference. Defendant's conduct constitutes violations of California Civil Code §§ 1798.81.5(a)(1) and 1798.150(a)(1) among other consumer protection statutes.

While this letter and the attached Complaint constitute sufficient notice of the claims asserted against Defendant, pursuant to California Civil Code 1798.150(b)(1), Plaintiff demands that, in the event a cure is possible, Defendant is hereby provided the opportunity to actually cure the noticed violations and provide Plaintiff with an express written statement within 30 days that the violations have been cured and that no further violations shall occur. A cure, if possible, requires that all the information taken has been recovered and that Plaintiff and the proposed class members of similarly situated persons are not at any risk of any of the information being used.

Thank you for your time and attention to this matter.

Sincerely,

s/ Abbas Kazerounian

Abbas Kazerounian, Esq.
KAZEROUNI LAW GROUP, APC
Direct Line: (800) 400-6808, Ext. 2
E-mail: ak@kazlg.com

[Enclosure]